

WHAT IS CLAIMED IS:

1. A verification result recording method for creating a verification log recording information about verification of a signature in a signature system including a signer side apparatus, a verifier side apparatus and a publishing organization side apparatus, wherein:

said signer side apparatus records a signature log entry relating to a signature created as a signer side signature log with a chain relation;

said publishing organization side apparatus publicizes said signature log entry deposited from said signer side apparatus, records a plurality of signature log entries deposited as a publishing organization side signature log with a chain relation and publicizes a predetermined signature log entry in said publishing organization side signature log as a newspaper publication signature log entry; and

said verifier side apparatus verifies matching of the chain relation among said signatures from said newspaper publication signature log entry to said signature log entry deposited by said signer side apparatus for publication by using said publishing organization side signature log, verifies matching of the chain relation among said signatures from said signature log entry deposited by said signer side apparatus for publication to said signature log entry relating to said verification object signature by using

said signer side signature log, and records the data used for said verification as a verification log.

2. A verification result recording method according to claim 1, wherein said data recorded in said verification log and utilized for said verification includes said verification object signature, said signer side signature log, said publishing organization side signature log and said newspaper publication signature log entry.

3. A verification result recording method according to claim 2, which includes the steps of:
extracting said verification object signature, said signer side signature log, said publishing organization side signature log and said newspaper publication signature log entry as the data utilized for said verification from said verification log;

verifying matching of the chain relation among said signatures from said newspaper publication signature log entry to said signature log entry relating to said verification object signature by utilizing said data utilized for said verification and so extracted; and

verifying said verification log.

4. A verifier side apparatus for executing signature verification, characterized by performing:

a reception processing for verifying a verification object signature by using a public key of

a signer;

a verification processing for verifying a chain relation from a newspaper publication signature log entry as a starting point to said verification object signature by using a signer side signature log and a publishing organization side signature log; and

a verification record preservation processing by creating a verification log from data used for said verification processing and recording said verification log.

5. A publishing organization side apparatus for executing a reliability improvement processing of a signature, characterized by performing:

a publication processing for publicizing a signature log entry deposited from a signer side apparatus;

a publication reminder processing for urging said signer side apparatus to publicize said signature log entry;

a publication notice processing for notifying said signer side apparatus of publication of a signature log entry deposited from other signer side apparatus; and

a verification vicarious execution processing for verifying a verification object signature by collecting data necessary for verification in place of said signer side apparatus, creating a verification log and notifying a verification result.

6. A publishing organization side apparatus according to claim 5, which executes, as said publication processing:

a publication processing for publicizing a signature log entry deposited from said signer side apparatus for publication;

a publication information registration processing for recording information relating to said signature log entry publicized;

a notice request existence/absence confirmation processing for confirming whether or not a publication notice request is received from other signer side apparatus as to said signature log entry publicized; and

a publication notice processing for giving a notice to said other signer side apparatus when said publication notice request is received as to said signature log entry publicized.

7. A publishing organization side apparatus according to claim 5, wherein said publication reminder processing executes:

an object extraction processing for specifying a signer to which publication of said signature log entry is to be urged:

a reminder transmission processing for transmitting a reminder document urging publication of said signature log entry to said signer side apparatus utilized by said signer specified; and

a reminder information registration processing for recording transmission of said reminder document.

8. A publishing organization side apparatus according to claim 5, wherein said publication notice processing executes:

a notice request content registration processing for receiving said publication notice request from said other signer side apparatus and registering the content of said publication notice request to said database;

a notice requesting party extraction processing for extracting information of said other signer side apparatus as a notice requesting party from said database registering the content of said notice request content; and

a notice transmission processing for notifying said other signer side apparatus as said notice requesting party of publication of said publication signature log entry by said notice requesting object signer.

9. A publishing organization side apparatus according to claim 5, wherein said verification vicarious execution processing executes:

a verification vicarious execution request reception processing for receiving a request of verification vicarious execution from said signer side apparatus;

a verification data collection processing for collecting a publication signature log entry and a signature log necessary for verification for said verification signature for which verification is requested;

a signature verification processing for verifying said verification signature for which verification is requested, by using the data collected by said verification data collection processing;

a verification log creation processing for creating a verification log recording said verification result and the data used for said verification and sending said verification log to said signer side apparatus as a verification requesting party;

a verification status registration processing for recording a verification status to said database for said verification object signature requested; and

a verification status confirmation processing for confirming said verification status for said verification vicarious execution processing requested.